

**CHENNAI – PONDICHERRY**

**Lightweight Fine-Grained Search over Encrypted Data in Fog Computing**

**Abstract**

Fog computing, as an extension of cloud computing, outsources the encrypted sensitive data to multiple fog nodes on the edge of Internet of Things (IoT) to decrease latency and network congestion. However, the existing ciphertext retrieval schemes rarely focus on the fog computing environment and most of them still impose high computational and storage overhead on resource-limited end users. In this paper, we first present a Lightweight Fine-Grained ciphertexts Search (LFGS) system in fog computing by extending Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Searchable Encryption (SE) technologies, which can achieve fine-grained access control and keyword search simultaneously. The LFGS can shift partial computational and storage overhead from end users to chosen fog nodes. Furthermore, the basic LFGS system is improved to support conjunctive keyword search and attribute update to avoid returning irrelevant search results and illegal accesses. The formal security analysis shows that the LFGS system can resist Chosen-Keyword Attack (CKA) and Chosen-Plaintext Attack (CPA), and the simulation using a real-world dataset demonstrates that the LFGS system is efficient and feasible in practice.